REMARKS

Claims 1, 3-10, 12-20, 22-26, 28-33, 35-39, 41-46, 48-51, and 53-70 are pending and remain in the application. Claims 1, 3, 10, 12, 19, 20, 22, 26, 28, 32, 33, 35, 39, 41, 45, 46, 48, 51, 53, and 56 have been amended. Claims 2, 11, 21, 27, 34, 40, 47, and 52 have been canceled. No new matter has been introduced.

Claims 41 and 68 stand rejected under 35 U.S.C. 112, first paragraph, as being not enabled. Applicant disagrees. The Specification at page 16, lines 20-22 recites that, "Each encrypted frame 221 is decrypted... using a private cryptographic key to create a decrypted frame 224," while at page 16, lines 24-27 the specification states, "As well, a digital signature 227 is authenticated... using a public cryptographic key 229 to re-create the cryptographic hash 230 generated from the original framed video content." Thus, at least these potions of the Specification are seen as enabling the recitations of Claim 41 and 68, which specify, "employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key." Withdrawal of the rejections under 35 U.S.C. 112, first paragraph, is respectfully requested.

Claims 1, 7, 8, 10, 16, 17, 20, 24-26, 30, 31, 33, 37-39, 43, 44, 49, 54, 59, 62, 66, and 69 stand rejected under 35 U.S.C. 102(b) as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 5,799,083, issued to Brothers et al. ("Brothers"). Applicant traverses the rejections.

A claim is anticipated under 35 U.S.C. §102(b) when each element specified by the claim is found in a single reference. *See, Crown Ops. Int'l., Ltd. v. Solutia Inc.*, 289 F.3d 1367 (Fed. Cir. 2002). Furthermore, the "single reference must describe the claimed invention with sufficient precision and detail to establish that the subject matter existed in the prior art." *Verve, LLC v. Crane Cams, Inc.*, 311 F.3d 1116 (Fed. Cir. 2002).

To establish a *prima facie* case of obviousness under 35 U.S.C. §103(a), the examiner has the burden of proving that (1) there is some suggestion or

motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there is a reasonable expectation of success; and (3) the combined references teach or suggest all the claim limitations. MPEP § 2143. Additionally, finding similar elements in one or more references does not render an invention automatically unpatentable, and the invention itself may not be used as an instruction book on how to reconstruct the invention from the art references. *See, Panduit Corp. v. Dennison, Mfg. Co.*, 810 F.2d 1561, 1 USPQ2d 1593 (Fed. Cir. 1987). Finally, obviousness may not be established by picking and choosing from an art reference only so much of the reference as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. *Bausch & Lomb, Inc. v. Barnes-Hind, Inc.*, 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986).

Brothers discloses an event verification system that includes a video camera for the reception of information, an encryption algorithm to encrypt the received information, an electronic recorder to record the encrypted information, a decryption algorithm to decrypt the recorded information, and at least one programmable memory to store at least one cryptographic key for use with the encryption and decryption algorithms. (Col. 2, ll. 43-49.) The input and at least one programmable memory in the camera are protected from access or alteration by means of a tamperproof enclosure. (Col. 2, ll. 49-51.) A trusted agent generates the cryptographic key and programs the cryptographic key into the programmable memory. (Col. 2, ll. 51-55.) In one embodiment, a single key encryption technique is used. (Col. 3, line 36.) Cryptographic integrity is provided by ensuring that the only two copies of the secret key are either in the possession of the trusted third party or resident in the memory in the tamperproof enclosure. (Col. 3, ll. 38-48.) In another embodiment, a public key event verification system is included. (Col. 5, line 61.) In this embodiment, a trusted third party creates a public/private key pair using a key generator and programs the camera with the public/private key pair. (Col. 5, ll. 64-67.)

Brothers provides authentication of a recording by two principal means. First, the trusted third party can be consulted to verify that the serial number of the camera correctly corresponds to the decrypted authorization code that was originally programmed into the camera by the manufacturer (Col. 5, ll. 34-48) or to obtain a public key from the trusted third party. (Col. 8. ll. 17-20.) Second, Brothers teaches providing authentication by periodically reprogramming the camera with a new key and key ID information by the trusted third party. (Col. 8, ll. 42-57.)

Independent Claims 1, 10, 20, 26, 33, 39, 46, and 51 have been amended to respectively incorporate the limitations recited by now-canceled dependent Claims 2, 11, 21, 27, 34, 40, 47, and 52. Support for the claim amendments can be found in the specification and claims as originally filed. In contrast to the teachings of the Brothers reference, amended Claim 1, taken as an example, recites an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium. Claim 1 further recites a decryption module retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption. Amended Claim 1 further recites a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form. Claim 1, as amended, further recites a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium. Finally, Claim 1, as amended, recites a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and

comparing the verification cryptographic hash and the original cryptographic hash. Amended Claims 10, 20, 26, 33, and 39 recite similar limitations. Original Claims 46, 51, 57, 60, 64, and 67 also recite similar limitations.

Brothers fails to teach or suggest an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium. Nor does Brother teach or suggest a decryption module retrieving encrypted frames from a transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption. Nor does Brothers teach or suggest a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form. Furthermore, Brothers fails to teach or suggest encrypting and decrypting individual frames and combining the decrypted frames in a playback frame buffer is described with sufficient precision and detail to establish that such subject matter exists in the prior art. Finally, Brothers fails to teach or suggest any form of authentication system or method involving generating an original cryptographic hash of fixed length and then verifying authenticity by generating a verification fixed length cryptographic hash. Accordingly, a *prima facie* case of anticipation under 35 U.S.C.§102(b) has not been shown with respect to Claims 1, 7, 8, 10, 16, 17, 20, 24-26, 30, 31, 33, 37-39, 43, 44, 49, 54, 59, 62, 66, and 69.

Nor does Brothers render Claims 1, 7, 8, 10, 16, 17, 20, 24-26, 30, 31, 33, 37-39, 43, 44, 49, 54, 59, 62, 66, and 69 obvious under 35 U.S.C. §103(a). Again, Brothers fails to teach or suggest encryption and decryption on a frame-by-frame basis. Brothers further fails to teach or suggest a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium. Nor does Brothers teach or suggest a verification module retrieving the digital signature from the transportable storage medium,

decrypting the encrypted original cryptographic hash into decrypted frames using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash. Thus, there is no suggestion or motivation in Brothers or in the knowledge generally available to one of ordinary skill in the art, to modify Brothers to contain such structure. Accordingly, a *prima facie* case of obviousness under 35 U.S.C. §103(a) has not been shown with respect to Claims 1, 10, 20, 26, 33, and 39.

Claims 7 and 8 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 16 and 17 are dependent on Claim 10 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 24 and 25 are dependent on Claim 20 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 30 and 31 are dependent on Claim 26 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 37 and 38 are dependent on Claim 33 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 43 and 44 are dependent on Claim 39 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 49 is dependent on Claim 46 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 54 is dependent on Claim 51 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 59 is dependent on Claim 57 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 62 is dependent on Claim 60 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 66 is dependent on Claim 64 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 69 is dependent on Claim 67 and is patentable for the above-stated reasons,

and as further distinguished by the limitations therein. Withdrawal of the rejection of Claims 1, 7, 8, 10, 16, 17, 20, 24-26, 30, 31, 33, 37-39, 43, 44, 49, 54, 59, 62, 66, and 69 under 35 U.S.C. §103(a) is respectfully requested.

Claims 2, 3, 5, 6, 9, 11, 12, 14, 15, 18, 19, 21-23, 27-29, 32, 34-36, 40-42, 45-48, 50-53, 55-58, 60, 61, 63-65, 67, 68, and 70 stand rejected under 35 U.S.C. §103(a) as being obvious over Brothers, in view of U.S. Patent No. 5,912,972, issued to Barton ("Barton").

To establish a *prima facie* case of obviousness under 35 U.S.C. §103(a), the examiner has the burden of proving that (1) there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there is a reasonable expectation of success; and (3) the combined references teach or suggest all the claim limitations. MPEP § 2143. Additionally, finding similar elements in one or more references does not render an invention automatically unpatentable, and the invention itself may not be used as an instruction book on how to reconstruct the invention from the art references. *See, Panduit Corp. v. Dennison, Mfg. Co.*, 810 F.2d 1561, 1 USPQ2d 1593 (Fed. Cir. 1987). Finally, obviousness may not be established by picking and choosing from an art reference only so much of the reference as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. *Bausch & Lomb, Inc. v. Barnes-Hind, Inc.*, 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986).

Barton discloses a method and apparatus for embedding authentication information within digital data. (Title) Arbitrary digital information is embedded with a stream of digital data so as to avoid detection by a casual observer and allow a user to determine whether the digital data have been modified from the intended form. (Abstract) Barton achieves this result by: (1) deliberately introducing errors into a digital data block to embed information into the block; (2) carefully choosing where the errors are introduced into the data block to avoid notice by casual observers; and (3) retrieving the embedded information on-

demand using proper knowledge of the error-inducing technique. (Col 11, ll. 1-12.) To further facilitate this technique, a compressed representation of the modified portions of the data block may be contained within the embedded information, in which case the original data block can be recovered by decompressing the representation and placing the correct bits into position within the block. (Col 11, ll. 13-19.) Any additional errors introduced into the digital data block after the embedding process are also detected. (Col. 11, ll.19-24.) By using appropriate algorithms, the information can be protected by either encrypting the information, including error correcting information, or through a combination of both techniques. (Col. 11, ll. 25-28.) Finally, the embedded information may include encoding that indicates the encryption technique used. (Col. 11, ll. 29-30.)

In contrast, Claim 1 as amended specifies a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium; and further specifies a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash into decrypted frames using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash. Amended Claims 10, 20, 26, 33, 39, 46, and 51 recite similar limitations. Original Claims 57, 60, 64, and 67 also recite similar limitations.

Neither Brothers nor Barton include any suggestion or incentive that their respective teachings be combined. Each reference provides an entirely independent system and method for authenticating a video recording. Brothers relies wholly on the integrity of a trusted third party to maintain accurate and confidential records of camera serial number and encryption codes. Barton relies on the carefully controlled and deliberate introduction of known errors into a data

block to embed information into the block and retrieving the embedded information on-demand using proper knowledge of the error-inducing technique. Moreover, Barton relies on carefully choosing where the errors are introduced into the data block to avoid notice by casual observers. Thus, the approaches used by Brothers and Barton are fundamentally different. Neither reference expressly nor inherently teaches or suggests any real or perceived difficulties or problems that would suggest combining the teachings of one reference with the other. Either approach is effective for its intended purpose standing alone. Thus, one skilled in the art would not reasonably perceive any need to combine the teachings of Brothers with those of Barton or vice versa.

Furthermore, there is no indication that combining the teachings of Brothers and Barton would result in a working system. On the contrary, combining the controlled error introduction technique of Barton with the teachings of Brothers would render the "trusted third party" both redundant and ineffective: redundant because the provision of the error introduction technique of Barton obviates the need for a trusted third party, and ineffective because, without knowledge of the error introduction protocol, the trusted third party would be unable to assist.

Finally, even if combined, Brothers and Barton do not result in the invention as claimed. In particular, neither Brothers nor Barton discloses generating a fixed-length original cryptographic hash from at least one individual frame. Nor does either reference disclose generating a verification fixed-length cryptographic hash. As a result, even if combined, the combination fails to compare fixed-length original and verifications cryptographic hashes. Accordingly, a *prima facie* case of obviousness has not been shown for Claims 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64, and 67.

By this Amendment, Claims 2, 11, 21, 27, 34, 40, 47, and 52 have been canceled and no longer remain in the applications. Claims 3, 5, 6, and 9 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 12, 14, 15, and 18 are

dependent on Claim 10 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 19 is multiply dependent on Claims 10, 12, 13, 14, 15, 16, 17, or 18 and is patentable for the above-stated reasons and as further distinguished by the limitations therein. Claims 22-23 are dependent on Claim 20 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 29 is dependent on Claim 26 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 32 is multiply dependent on Claims 26, 28, 29, 30, or 31 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 35-36 are dependent on Claim 33 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 41-42 are dependent on Claim 39 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 45 is multiply dependent on Claims 39, 41, 42, 43, or 44 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 48, and 50 are dependent on Claim 46 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 53, and 55 are dependent on Claim 51 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 56 is multiply dependent on Claims 51, 54 or 55 and is patentable for the above stated reasons, and as further distinguished by the limitations therein. Claim 58 is dependent on Claim 57 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 61 is dependent on Claim 60 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 63 is multiply dependent on Claims 60, 61, or 62 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 65 is dependent on Claim 64 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 68 is dependent on Claim 67 and is patentable for the above-stated reasons, and as further distinguished by the

limitations therein. Claim 70 is multiply dependent on Claims 67, 68, or 69 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection of Claims 2, 3, 5, 6, 9, 11, 12, 14, 15, 18, 19, 21-23, 27-29, 32, 34-36, 40-42, 45-48, 50-53, 55-58, 60, 61, 63-65, 67, 68, and 70 under 35 U.S.C. §103(a) is respectfully requested.

Claims 4, 13, and 19 stand rejected under 35 U.S.C. §103(a) as being obvious over Brothers, in view of U.S. Patent Application Publication No. US 2002/0112168A1 hereinafter referred to as Filipi-Martin.

Claim 4 depends from amended independent Claim 1, while Claims 13 and 19 each ultimately depend from amended independent Claim 10. In view of the amendments to Claims 1 and 10 and the arguments presented above, the rejection of Claims 4, 13, and 19 in view of Filipi-Martin has been obviated and withdrawal of the rejection of Claims 4, 13, and 19 under 35 U.S.C. §103(a) is respectfully requested.

Examination and further consideration of the application is respectfully requested. Non-canceled Claims 1, 3-10, 12-20, 22-26, 28-33, 35-39, 41-46, 48-51, and 53-70 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: February 24, 2005

By: _____
Patrick J.S. Inouye, Esq.
Reg. No. 40,297

Law Offices of Patrick J.S. Inouye
810 Third Avenue, Suite 258
Seattle, WA 98104

Telephone: (206) 381-3900
Facsimile: (206) 381-3999